Procédure de gestion des incidents de confidentialité

Définitions

Incident de sécurité
Incident qui affecte la confidentialité, la disponibilité ou l'intégrité des informations d'un système ou la continuité de service de l'Externat St-Jean-Berchmans, incluant ou non des renseignements personnels.

Incident de confidentialité
Accès, utilisation et communication non autorisé(e) par la loi d'un renseignement personnel, perte d'un tel renseignement ou toute autre atteinte à la protection de celui-ci.

Renseignements personnels
Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier.

Plan d'intervention

Dans le contexte de la Loi 25, ce plan d'intervention a pour objectif d'identifier les intervenants, les étapes, les démarches et les actions requises en vue de s'assurer que les incidents impliquant les Renseignements personnels détenus par l'Externat St-Jean-Berchmans soient traités de manière coordonnée, efficiente et rapide, afin d'atténuer les risques susceptibles d'en découler et d'apporter les correctifs nécessaires ».

Ce plan vise tout le personnel de l'Externat St-Jean-Berchmans ainsi que les tiers avec qui l'Externat St-Jean-Berchmans fait affaire.

Le responsable de la protection des données personnelles ainsi que la responsable de l'accès aux données personnelles veillent à la mise en œuvre et au respect de ce plan d'intervention.

En cas d'incident, voici les membres de l'équipe de réponse au sein de l'Externat St-Jean-Berchmans qui devront être contactés selon le rôle et les responsabilités de chacun.

Rôle	Nom	Titre	Téléphone	Courriel
Interne				
Responsable de la gestion des incidents	Marie-Eve Potvin	Directrice générale	418 687-5871 poste 222	marie-eve.potvin@externatsjb.com
Responsable de la protection des renseignements personnels	Luc Deslauriers	Technicien informatique	418 687-5871 poste 235	luc.deslauriers@externatsjb.com
Responsable TI / sécurité	Luc Deslauriers	Technicien informatique	418 687-5871 poste 235	luc.deslauriers@externatsjb.com

Lorsqu'un incident de sécurité ou de confidentialité est constaté, il faut immédiatement communiquer avec le responsable de la gestion des incidents de sécurité, qui verra à mettre en œuvre le plan d'intervention et impliquer les membres de l'équipe et toute autre personne susceptible d'aider à diminuer le risque.

Sous la direction de l'équipe de gestion des incidents, l'établissement doit tout d'abord identifier l'incident concerné, autant que possible. À cette fin, il doit déterminer et documenter :

- La cause et l'origine de l'incident (date, heure, lieu, support, cause interne ou externe, personne responsable, déterminer si l'incident est terminé ou en cours)
- Les renseignements visés (personnels ou non), leur nombre et les personnes concernées.

L'établissement doit entreprendre immédiatement des mesures pour contenir les effets de l'incident et prévenir des impacts négatifs additionnels pour lui ou des tiers. Les mesures entreprises seront documentées. La nature de ces mesures dépendra du type d'incident en cause. Ainsi, on ne réagira pas de la même manière à une cyber-attaque qu'à un courriel transmis par erreur à un mauvais destinataire.

À cette étape, l'Externat St-Jean-Berchmans pourra notamment considérer les éléments suivants :

- Contenir la menace par le confinement / isolement des composants affectés
- Modifier (révoquer) les accès et mots de passe si requis
- Identifier, localiser et préserver les renseignements visés par l'incident
- Protéger la confidentialité des renseignements personnels visés
- Récupérer les renseignements personnels / les supports – obtenir une confirmation de destruction / de non-diffusion du responsable de l'incident
- Empêcher la diffusion / la divulgation des renseignements – chiffrement, blocage des accès
- Conserver tous les documents en place au moment de l'incident sans les modifier, notamment pour préserver la preuve

Une fois l'incident identifié et contenu, une enquête plus approfondie sera effectuée pour déterminer et documenter, aussi précisément que possible

- La cause et l'origine de l'incident
- Les renseignements visés (personnels ou non) ainsi que leur nombre
- Les personnes visées, le cas échéant, et leur emplacement géographique
- Le risque de préjudice pour les personnes concernées selon la grille d'analyse du préjudice

L'Externat St-Jean-Berchmans mettra en place un protocole, tant à l'interne qu'à l'externe, pour communiquer sur l'incident de confidentialité.

- Aviser le personnel
- Insister sur le fait que l'incident n'a pas encore été révélé à l'externe
- Indiquer jusqu'à quelle date il y a un embargo
- Avis aux autorités (Commission d'accès à l'information ou autres autorités réglementaires pertinentes, service de police, etc.)
- Avis aux personnes concernées
    - Si l'établissement décide de ne pas le faire, les raisons conduisant à cette décision seront documentées.
- Avis aux médias / communiqué de presse

L'Externat St-Jean-Berchmans précisera les éléments qui seront pris en considération afin de continuer les activités mais aussi afin de faire un suivi (post-mortem) sur l'incident pour éviter que pareille situation ne se reproduise.

- Effectuer un post-mortem pour identifier et examiner les leçons tirées de l'incident ainsi que les domaines à améliorer
- Faire un suivi interne des mesures de sécurité, des politiques / procédures adoptées / révisées à la suite de l'incident
- Possibilité de faire appel à un audit externe pour évaluer les mesures de sécurité ; politiques / procédures adoptées / révisées à la suite de l'incident
- Considérer la mise en place d'un service de surveillance de crédit (Équifax, TransUnion, par ex.)
- Prévoir la stratégie pour réduire le risque de poursuite judiciaire et la stratégie de défense en cas de poursuite judiciaire
- Enregistrer l'incident dans le registre des incidents de confidentialité
- Revoir la couverture d'assurance
- Formation, sensibilisation
- Communication pour reconstruire la confiance tant à l'interne qu'à l'externe